REMARKS

Claims 1-6, 8-19, and 21-24 are pending in the application, of which Claims 1 and 17 are independent. All claims have been rejected under 35 U.S.C. 103(a). Those rejections are respectfully traversed and reconsideration is requested.

Rejections Under 35 U.S.C. 103(a)

Claims 1-6, 8-19, and 21-24 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Belfiore *et al.* (U.S. Patent No. 6,990,513, hereinafter "Belfiore") in view of Ginter *et al.* (U.S. Patent No. 7,165,174, hereinafter "Ginter").

Summary of Application and Cited References

Before discussing the cited references, a brief review of the Applicants' disclosure may be helpful without limiting the claims. The Applicants' disclosure is directed to a method and system for providing a usage accountability model for data security in a data processing system. Referring to Figs. 2 and 3 of the Applicants' specification, an agent process 300 runs in the background of a client operating system kernel 102 and interrupts requests for access to digital assets (e.g., data files) at a point of authorized access to the assets. The agent process 300 contains sensors 500 that capture low-level (atomic) system events 350, 510, such as file read, file write, clipboard copy, CD-RW access, TCP/IP network message outbound, and the like. The atomic events 350, 510 are then associated with one or more file names, and a filter 520 filters the atomic events 350, 510 against an approved list, removing atomic events that are associated with approved files (such as operating system files) that likely do not contain sensitive application data. A coalescer 530 further processes the atomic events 350, 510 associated with, or related to, a single user action. For example, a typical pattern of file access is a "file open" atomic event followed by multiple "file read" atomic events to the same file. If such a sequence of atomic events 350, 510 occurs from the same process and the same executable with the same thread ID and the same file name, the coalescer 530 considers the multiple atomic events as being only a single "file open" atomic event. The resulting events are then sent to a journaling server 104-2, which examines the events to determine the occurrence of an aggregate event 360, the presence of which may indicate an abuse of authorized access to the digital asset(s). For

example, an aggregate "FileEdit" event may be reported by the journaling server 104-2 if a user has opened and modified a sensitive financial document, with that user then printing the document, renaming it, and saving it to a newly attached USB hard drive. As illustrated in Figs. 6A-6C, a set of reports are then generated based on the aggregate events, which provide an understanding of how files have been accessed, used, and communicated by various end users of the data processing system. The reports serve as an audit trail that may be used to determine possible abuses of authorized access to the digital assets (e.g., data files).

Turning to the cited reference, Belfiore presents a method and system for facilitating improved communications and collaboration across computer networks consisting of client devices and multiple servers. One particular component of Belfiore is an event component, which is used to synchronize events and provide notification about certain activities within the system. The event component includes an event composition mechanism that transforms atomic level events into progressively higher level events based on rules, filters, and pattern recognizers. These events (of varying levels) are passed between software components at various locations in the computer network. Upon receiving an event, the receiving software component may perform a particular action based on the received event. For example, the receipt of a certain event may cause an administrator of the network to receive an urgent notification that a server of the network has failed. Also, while Belfiore includes a security component that may control how the events are communicated, it should be stressed that the events of Belfiore are not used to control network security.

Cited reference Ginter discloses a system for providing services for electronic commerce. The system includes a variety of components, such as a "usage clearinghouse," which has been cited by the Office in the present rejection. With regard to the usage clearinghouse, and referring to Fig. 35 of Ginter, a provider 164 may provide an electronic property (e.g., a movie over the Internet) 166 to one or more consumers 95. As the consumers 95 use the property (e.g., access the movie), audit trails 302 are generated based on the consumers' usage of the property 166. Upon the occurrence of a particular event (e.g., a point in time or number of uses of the property), the audit trails 302 are sent to the usage clearinghouse 300. The usage clearinghouse 300 then generates a report 304 based on the received audit trails 302 and sends the report 304 to

the provider 164, which may be used by the provider to collect payments from the consumers for their use of the electronic property. (*See* Ginter, col. 65, lines 4-34.)

Independent Claims 1 and 17

The Office states on page 5 of the Office Action that Belfiore does not disclose *"a reporter to generate an audit trail from the at least one aggregate event, the audit trail representing usage of the at least one digital asset by the end user,"* as recited in Claim 1 and as similarly recited in Claim 17. The Office also asserts that the usage clearinghouse of Ginter cures Belfiore's deficiency. Applicants respectfully disagree.

While the audit trails of Ginter represent the usage of the electronic property by the consumers, Ginter does not disclose that the audit trails are generated from *"at least one aggregate event,"* as claimed in independent Claims 1 and 17. As described in the Applicants' specification, an aggregate event is a particular type of event that corresponds to a certain predetermined sequence of atomic level events (*see* Applicants' specification, page 7, lines 14-20). Ginter does refer to a sort of aggregation, in that payments in the system of Ginter are aggregated, but the aggregation of payments is not equivalent to the aggregate events of the present application and, as such, Ginter discloses no such aggregate events. To interpret any aggregation in Ginter as disclosing the claimed *"aggregate events"* would be inconsistent with the Applicants' specification. Therefore, because Ginter discloses no such aggregate events, Ginter cannot generate an audit trail from such aggregate events.

Moreover, even if Ginter did disclose the generation of an audit trail from aggregate events, the generation of the audit trail does not take place at a central location. In Ginter, the audit trails are generated at each of the consumers' locations, and sent to the usage clearinghouse. In contrast, the audit trail of the present application is generated at the journaling server (i.e., a central location) after the journaling server receives the atomic level events from the user client devices. Because Ginter does not disclose that the audit trails are generated from aggregate events and because the audit trails of Ginter are not generated at a central location (i.e., at a location equivalent to the journaling server of the claimed invention), Ginter does not disclose *"a journaling server ... having a reporter to generate an audit trail from the at least one aggregate event, the audit trail representing usage of the at least one digital asset by the end user,"* as claimed in Claim 1 and as similarly claimed in Claim 17.

Furthermore, there is no suggestion or motivation to combine the Belfiore and Ginter references. The Office asserts on pages 5 and 6 of the Office Action that it would have been obvious to combine the features of Ginter into the method of Belfiore "for the purpose of building a data security model which includes usage information while at the same time aggregating and providing a high level of accountability." The Office cites column 57, lines 9-11 of Ginter in support of the assertion; therefore, the Office has asserted that the motivation to combine Ginter with Belfiore is found in the cited portion of Ginter. According to the above quoted statement, the Office asserts that Ginter provides a motivation to modify Belfiore for the purpose of building a data security model; however, the cited portion of Ginter is concerned with a usage clearinghouse and, as described above, the usage clearinghouse relates to tracking usage of electronic properties for payment purposes, not data security.

According to the Office's statement, the Office also asserts that Ginter provides a motivation to provide usage information while at the same time aggregating (i.e., aggregating events) and providing a high level of accountability (i.e., usage accountability for data security); however, this is not the case, as the cited portion of Ginter reads "This ability to separately handle and process more detailed and granular usage information while at the same time aggregating payments can provide a high level of auditing accountability without unduly burdening the payment handling mechanism." As is apparent from the cited portion of Ginter, the aggregation is not of atomic level events according to a predetermined sequence of events, but is of payments within the system of Ginter. Also, despite the presence of the word "accountability," the cited portion does not provide any motivation to build an accountability model for data security.

Therefore, Applicants respectfully submit that the motivation provided by the Office for combining Ginter with Belfiore is not proper. Furthermore, as presented above, even if combined, Ginter and Belfiore do not result in the claimed invention. As such, independent Claims 1 and 17 are believed to be novel and nonobvious over the cited art.

Dependent Claims

Dependent Claims 2-6, 8-16, 18, 19, and 21-24 depend from either Claims 1 or 17 and, thus, include the elements of either Claims 1 or 17 presented above as being novel and nonobvious over the cited art. Therefore, Applicants respectfully submit that dependent Claims

2-6, 8-16, 18, 19, and 21-24 are novel and nonobvious over the cited art for at least the same reasons as presented above for independent Claims 1 and 17.

Furthermore, dependent Claims 2-6, 8-16, 18, 19, and 21-24 recite further elements that are neither taught nor suggested by the cited or prior art. For example, the combination of Belfiore and Ginter does not teach or suggest *"coalescing at least some of the atomic events into a single event"* as claimed in Claim 8 and as similarly claimed in Claim 21. In the Applicants' specification, coalescing is defined as the combination of a number of related atomic events into a single atomic event, such as, for example, the combination of a "file open" atomic event followed by multiple "file read" atomic events to the same file. This is different than the meaning of event aggregation, as the multiple atomic level events are not aggregated into a higher level event, but coalesced into a single atomic (low level) event. In the above example, the "file open" event and multiple "file read" events will be combined into a single "file open" atomic event.

Neither Belfiore nor Ginter discloses such a coalescer. The Office has indicated only reference numeral 606 of Fig. 5 as disclosing the Applicants' claimed coalescer; however, reference numeral 606 refers only to the multiple events of Belfiore being sent to Belfiore's event composition mechanism, and not being coalesced as described above. A mere indication that multiple events are passed from one component to another does not disclose the intricate details of the claimed coalescer. Nothing in Ginter cures Belfiore's deficiency. Because Belfiore and Ginter, taken either separately or in combination, do not disclose the coalescing of multiple atomic event into a single atomic event, dependent Claims 8 and 21 are believed, in addition to the reasons presented above for Claims 1 and 17, to further distinguish over the cited references.

Claim 13, which depends from Claim 8, recites that *"the coalescer reports a single coalesced event after a time out period with no activity."* The Office asserts that Belfiore's disclosure regarding a notification when "there is no mouse movement and no key is pressed in 5 minutes" serves to disclose the subject matter claimed in Claim 13 (*see* Belfiore, col. 24, lines 21-22); however, given the definition of a coalesced event as described above, such a statement cannot be interpreted to disclose the subject matter of Claim 13, as it does not recite reporting a coalesced event. Nothing in Ginter cures Belfiore's deficiency. Therefore, in addition to the

reasons presented above for Claims 1 and 17, dependent Claim 13 is believed to further distinguish over the cited references.

As a further example, the combination of Belfiore and Ginter does not teach or suggest *"control[ling] security of the data processing system by determining patterns of unexpected behavior based on the at least one aggregate event and the audit trail"* as claimed in Claim 14. It should be noted that while Belfiore includes a security component that may control how the events of Belfiore are communicated, the events of Belfiore are not used to control network security. Additionally, the usage clearinghouse of Ginter is also not used to control security. Furthermore, neither Belfiore nor Ginter disclose determining patterns of unexpected behavior based on aggregate events and an audit trail. Thus, because neither the events of Belfiore nor the audit trails of Ginter are used to control security and are not used to determine patterns of unexpected behavior, Belfiore and Ginter, taken either separately or in combination, cannot disclose the Applicants' invention as claimed in Claim 14. Therefore, in addition to the reasons presented above for Claims 1 and 17, dependent Claim 14 is believed to further distinguish over the cited references.

As yet a further example, the combination of Belfiore and Ginter does not teach or suggest *"provid[ing] a perimeter of accountability for usage of the at least one digital asset"* as claimed in Claim 15. Belfiore does not disclose a perimeter of accountability for usage of any of its assets. While Ginter may disclose tracking the usage of electronic properties, Ginter does not disclose such a perimeter for doing so. Thus, neither Belfiore nor Ginter determines accountability for asset usage outside such a perimeter of accountability. Therefore, Belfiore and Ginter, taken either separately or in combination, cannot disclose the Applicants' invention as claimed in Claim 15.

As yet a further example, the combination of Belfiore and Ginter does not teach or suggest that *"the accountability is of access, modification, and distribution"* of the digital assets, as claimed in dependent Claim 16, and does not teach or suggest that the usage of the digital assets *"includes access and dissemination"* of the digital assets, as claimed in dependent Claims 23 and 24. While Ginter discloses the tracking of usage of electronic properties by consumers (in the form of accessing the property), Ginter does not disclose that the consumers may modify, distribute, or disseminate the electronic property, or more particularly, that such activity is

tracked. Thus, Ginter does not disclose accountability that is of access, modification, and distribution, and does not disclose that usage of the electronic properties include access and dissemination. Nothing in Belfiore cures Ginter's deficiency. Therefore, in addition to the reasons presented above for Claims 1 and 17, Claims 16, 23, and 24 are believed to further distinguish over the cited references.

As such, the rejections of Claims 1-6, 8-19, and 21-24 under 35 U.S.C. 103(a) are believed to be overcome. Withdrawal of those rejections is respectfully requested.

Accordingly, the present invention as claimed is not believed to be anticipated or made obvious by the cited or prior art. Acceptance of Claims 1-6, 8-19, and 21-24 is respectfully requested.

CONCLUSION

In view of the above remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By _____

Patrick A. Quinlan
Registration No. 61,287
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133

Date: 2/25/08